IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

MASAYOSHI KAWAMOTO et al.

Group Art Unit: 2437

Examiner: Abyaneh, Ali S

Serial No.: 10/517,933

Filed: August 15, 2005

For: CARD ISSUING SYSTEM AND CARD ISSUING METHOD

Attorney Docket No.: IKU 0112 PUSA (JCB-001-PCT-US)

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief for the appeal from the final rejection of claims 21-36 of the final Office Action mailed June 18, 2009 for the above-identified patent application.

The fee of $540.00 as applicable under the provisions of 37 C.F.R. § 41.20(b)(2) is being charged to our Deposit Account No. 02-3978 via electronic authorization submitted concurrently herewith. Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

I. REAL PARTY IN INTEREST

The real party in interest is JCB Co., Ltd ("the Assignee"), a company organized and existing under the laws of Japan and having a place of business at 1-22 Minami Aoyama 5-chome, Minato-ku, Tokyo, Japan 107-8686, as set forth in the assignment recorded in the U.S. Patent and Trademark Office on August 15, 2005 at Reel 016882 / Frame 0078.

II. RELATED APPEALS AND INTERFERENCES

There are no appeals, interferences or judicial proceedings known to the Appellant (i.e., "the Applicant"), the Appellant's legal representative, or the Assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 21-36 are pending in this application. Claims 1-20 have been cancelled. Claims 21-36 have been finally rejected in the final Office Action mailed June 18, 2009. Claims 21, 25, 29, and 33 are independent claims.

Claims 21-36 are being appealed. (A copy of claims 21-36 is set forth in the attached Claims Appendix as these claims are involved in this appeal.)

IV. STATUS OF AMENDMENTS

No amendments were filed after the final Office Action mailed June 18, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

1. Independent Claim 21

Independent claim 21 recites a card issuing system for issuing an integrated chip ("IC") card (23). (Figs. 1 and 2; and page 3, lines 14-30; page 8, lines 8-19; and page 10, lines 9-13 of the specification.)

The card issuing system includes a card issuing center (1) having a center communication means (11) for transmitting card writing data. The card writing data includes at least one of a card number and personal information. (Fig. 1; and page 10, lines 14-25; page 11, lines 15-30; and page 13, lines 4-8 of the specification.)

The card issuing system further includes a base (2). The base (2) has a card communication mediate means (211) for receiving the card writing data from the center communication means (11) via a network (3). The base (2) has a card writer (22) for receiving an IC card (23). The base (2) has a cipher decoding means (212) in communication with the card communication mediate means (211) and the card writer (22). The cipher decoding means (212) has an access key (213). (Fig. 1; and page 10, line 14 – page 11, line 4; page 13, line 15 – page 14, line 25; and page 16, lines 4-9 of the specification.)

While the card writer (22) receives an IC card (23) having an access key, the cipher decoding means (212) is operable for determining whether the access key of the IC card (23) and the access key (213) of the cipher decoding means (212) correspond to one another. (Fig. 1; and page 14, lines 16-22; and page 18, line 24 – page 19, line 5 of the specification.) If the access keys correspond to one another, the cipher decoding means (212) is further operable for enabling the card communication mediate means (211) to receive the card writing data from the center communication means (11) and transmit the received card writing data to the card writer (22) for the card writer (22) to write the card writing data to the IC card (23) such that the

card writing data is transmitted from the card issuing center (1) to the IC card (23) without being stored in the base (2) thereby securing security of the at least one of the card number and the personal information of the card writing data. (Figs. 1 and 2 (blocks S250, S260, S270, and S280); and page 3, lines 14-30; page 8, lines 8-19; page 14, lines 11-25; page 15, lines 2-9; page 16, lines 4-15; page 18, line 23 – page 19, line 25 of the specification.)

2. Independent Claim 25

Independent claim 25 recites a card issuing method for issuing an integrated chip ("IC") card (23). (Figs. 1 and 2; and page 3, lines 14-30; page 8, lines 8-19; and page 10, lines 9-13 of the specification.)

The method includes providing a card issuing center (1) having a center communication means (11) for transmitting card writing data. The card writing data includes at least one of a card number and personal information. (Fig. 1; and page 10, lines 14-25; page 11, lines 15-30; and page 13, lines 4-8 of the specification.)

The method includes providing a base (2) having a card communication mediate means (211) for receiving the card writing data from the center communication means (11) via a network (3), a card writer (22) for receiving an IC card (23), and a cipher decoding means (212) in communication with the card communication mediate means (211) and the card writer (22), the cipher decoding means (212) having an access key (213). (Fig. 1; and page 10, line 14 – page 11, line 4; page 13, line 15 – page 14, line 25; and page 16, lines 4-9 of the specification.)

The method includes, while the card writer (22) receives an IC card (23) having an access key, determining by the cipher decoding means (212) whether the access key of the IC card (23) and the access key (213) of the cipher decoding means (212) correspond to one another. (Fig. 1; and page 14, lines 16-22; and page 18, line 24 – page 19, line 5 of the specification.) If the access keys correspond to one another, the method further includes enabling by the cipher decoding means (212) the card communication mediate means (211) to receive the card writing data from the center communication means (11) and transmit the received card writing data to the card writer (22) for the card writer (22) to write the card writing data to the IC card (23) such that the card writing data is transmitted from the card issuing center (1) to the IC card (23) without being stored in the base (2) thereby securing security of the at least one of the card number and the personal information of the card writing data. (Figs. 1 and 2 (blocks S250, S260,

S270, and S280); and page 3, lines 14-30; page 8, lines 8-19; page 14, lines 11-25; page 15, lines 2-9; page 16, lines 4-15; page 18, line 23 – page 19, line 25 of the specification.)

3. Independent Claim 29

Independent claim 29 recites a card issuing system for issuing an integrated chip ("IC") card (23). (Figs. 1 and 2; and page 3, lines 14-30; page 8, lines 8-19; and page 10, lines 9-13 of the specification.)

The card issuing system includes a card issuing center (1) having a center communication means (11) for transmitting card writing data. The card writing data includes at least one of a card number and personal information. (Fig. 1; and page 10, lines 14-25; page 11, lines 15-30; and page 13, lines 4-8 of the specification.)

The card issuing system includes a base (2) having a card communication mediate means (211) for receiving the card writing data from the center communication means (11) via a network (3) and a card writer (22) for receiving an IC card (23). (Fig. 1; and page 10, line 14 – page 11, line 4; and page 13, line 15 – page 14, line 10 of the specification.)

While the card writer (22) receives an IC card (23) having an access key during a communication connection between the center communication means (11) and the card communication mediate means (211), the card issuing center (1) is operable for accessing the access key of the IC card (23) and determining whether the IC card (23) is authenticated based on the access key of the IC card (23). (Fig. 1; and page 14, lines 16-22; and page 15, lines 10-23 of the specification.) If the IC card (23) is authenticated, the card issuing center (1) being further operable for enabling the card communication mediate means (211) to receive the card writing data from the center communication means (11) and transmit the received card writing data to the card writer (22) for the card writer (22) to write the card writing data to the IC card (23) such that the card writing data is transmitted from the card issuing center (1) to the IC card (23) without being stored in the base (2) thereby securing security of the at least one of the card number and the personal information of the card writing data. (Figs. 1 and 2 (blocks S250, S260,

S270, and S280); and page 3, lines 14-30; page 8, lines 8-19; page 14, lines 11-25; and page 15, lines 2-23 of the specification.)

4. Independent Claim 33

Independent claim 33 recites a card issuing method for issuing an integrated chip ("IC") card (23). (Figs. 1 and 2; and page 3, lines 14-30; page 8, lines 8-19; and page 10, lines 9-13 of the specification.)

The method includes providing a card issuing center (1) having a center communication means (11) for transmitting card writing data. The card writing data includes at least one of a card number and personal information. (Fig. 1; and page 10, lines 14-25; page 11, lines 15-30; and page 13, lines 4-8 of the specification.)

The method includes providing a base (2) having a card communication mediate means (211) for receiving the card writing data from the center communication means (11) via a network (3) and a card writer (22) for receiving an IC card (23). (Fig. 1; and page 10, line 14 – page 11, line 4; and page 13, line 15 – page 14, line 10 of the specification.)

The method includes, while the card writer (22) receives an IC card (23) having an access key during a communication connection between the center communication means (11) and the card communication mediate means (211), accessing by the card issuing center (1) the access key of the IC card (23) and determining by the card issuing center (1) whether the IC card (23) is authenticated based on the access key of the IC card (23). (Fig. 1; and page 14, lines 16-22; and page 15, lines 10-23 of the specification.) If the IC card (23) is authenticated, the method further includes enabling by the card issuing center (1) the card communication mediate means (211) to receive the card writing data from the center communication means (11) and transmit the received card writing data to the card writer (22) for the card writer (22) to write the card writing data to the IC card (23) such that the card writing data is transmitted from the card issuing center (1) to the IC card (23) without being stored in the base (2) thereby securing security of the at least one of the card number and the personal information of the card writing data. (Figs. 1

and 2 (blocks S250, S260, S270, and S280); and page 3, lines 14-30; page 8, lines 8-19; page 14, lines 11-25; and page 15, lines 2-23 of the specification.)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 21-36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,534,857 to Laing et al. ("Laing") in view of U.S. Patent No. 6,336,585 to Harada ("Harada").

VII. ARGUMENT

A. Claims 21-36 are Patentable under 35 U.S.C. §103(a) over U.S. Patent No. 5,534,857 (Laing) in view of U.S. Patent No. 6,336,585 (Harada)

1. The Independent Claims

Independent claims 21, 25, 29, and 33 are directed to systems and methods for issuing an integrated chip ("IC") card in an environment having a card issuing center and a base. The card issuing center has a center communication means for transmitting card writing data ("data") including at least one of a card number and personal information. The base has a card communication mediate means for receiving the data from the center communication means via a network. The base also has a card writer for receiving an IC card.

As set forth in independent claims 21 and 25, the base further has a cipher decoding means in communication with the card communication mediate means and the card writer. The cipher decoding means has an access key. While the card writer receives an IC card having an access key, the cipher decoding means determines whether the access key of the IC card and the access key of the cipher decoding means correspond to one another. If the access keys correspond to one another, the cipher decoding means enables the card communication mediate means to receive the data from the center communication means and transmit the received data to the card writer for the card writer to write the data to the IC card such that the data is transmitted from the card issuing center to the IC card without being stored in the base thereby securing security of the at least one of the card number and the personal information of the data.

As set forth in independent claims 29 and 33, while the card writer receives an IC card having an access key during a communication connection between the center communication means and the card communication mediate means, the card issuing center accesses the access key of the IC card and determines whether the IC card is authenticated based

on the access key of the IC card. If the IC card is authenticated, the card issuing center enables the card communication mediate means to receive the data from the center communication means and transmit the received data to the card writer for the card writer to write the data to the IC card such that the data is transmitted from the card issuing center to the IC card without being stored in the base thereby securing security of the at least one of the card number and the personal information of the data.

2. Laing in view of Harada

The Examiner posited that Laing teaches a card issuing system for issuing an IC card, the system comprising: a card issuing center having a center communication means for transmitting card writing data ("data") including at least one of a card number and personal information (citing col. 1, lines 62-65 and col. 3, lines 22-27); and a base having a card communication mediate means for receiving the data from the center communication means via a network, a card writer for receiving an IC card, and a cipher decoding means in communication with the card communication mediate means and the card writer, the cipher decoding means has an access key (citing col. 3, lines 29-59); the cipher decoding means enabling the card communication mediate means to receive the data from the center communication means and transmit the received data to the card writer for the card writer to write the data to the IC card such that the data is transmitted from the card issuing center to the IC card without being stored in the base thereby securing security of the at least one of the card number and the personal information of the data (col. 6, line 45 – col. 7, line 14).

The Examiner indicated that Laing does not explicitly teach wherein while the card writer receives an IC card having an access key, the cipher decoding means being operable for determining whether the access key of the IC card and the access key of the cipher decoding means correspond to one another.

The Examiner posited that Harada teaches determining whether the access key of the IC card and the access key of the cipher decoding means correspond to one another (citing col. 8, lines 5-60).

3. The Independent Claims Compared to Laing in view of Harada

Independent claims 21, 25, 29, and 33 include features directed to enabling a transfer of data from a card issuing center to a base for the base to write the data into an IC card at the base, in which the IC card is an entity that is to receive data to be written thereto, upon determining that the IC card is authenticated. That is, a transfer of data from the center to the base, for the base to write the data to an IC card at the base, is enabled upon determining that the IC card is authenticated. In this way, the data is transmitted from the center to the IC card without being stored in the base thereby securing security of the data.

As set forth in independent claims 21 and 25, the base controls as to whether the center is to transfer data to the base for the base to write to the IC card. To this end, while a card writer at the base receives the IC card, a cipher decoding means of the base determines whether the IC card is authenticated by comparing an access key of the IC card with an access key of the cipher decoding means. If the two access keys correspond (i.e., if the IC card is authenticated), then the cipher decoding means enables the base to receive the data from the center and transmit the data to the writer for the writer to write the data to the IC card.

As set forth in independent claims 29 and 33, the center controls as to whether the center is to transfer data to the base for the base to write to the IC card. To this end, while a card writer at the base receives the IC card during a communication connection between the center and the base, the center accesses an access key of the IC card and determines whether the IC card is authenticated based on the access key of the IC card. If the IC card is authenticated, then the center enables the base to receive the data from the center and transmit the data to the writer for the writer to write the data to the IC card.

Laing is directed to enabling a transfer of data from a central administration system (i.e., a card issuing center) (2; 5) to a retailer system (i.e., a base) (3; 6, 7, 8) upon the center and the base authenticating one another. To this end, upon the center and the base authenticating one another, a session key is established and the session key is used in transferring data from the center to an IC card (9) at the base. (See, for example, the abstract, "The retailer is authenticated to the issuer and the issuer to the retailer . . . A session key is established for enciphering data traffic between the secure terminal device [7] and the issuer's computer [5] . . . The customer smart card [9] is presented to the secure terminal device. Confidential customer data is enciphered using the session key and it is written from the issuer's computer to the customer smart card."; col. 5, lines 27-28, "Once both the Central Administration System and the Retailer System have authenticated each other, they can mutually establish session keys for enciphering future data traffic between them."; col. 7, lines 11-13, "Information in steps 80, 82 can be transmitted between the customer's smart card, C2 and the issuer's secure computer after enciphering and deciphering using the session key.")

Harada is directed to "checking a memory card for authenticity before executing an application program stored in the memory card" (col. 1, lines 65-67). The memory card (5) and an IC card (20) are within electronic equipment (13). The electronic equipment checks the memory card for authenticity, and if the memory card is authentic, then the electronic equipment reads an application program (AP 2) stored in the memory card and carries out an electronic transaction involving the IC card according to the application program (AP 2). (Fig. 3; col. 3, lines 57-61; col. 8, lines 20-65).

The independent claims differ from Laing in view of Harada in that the independent claims include features directed to enabling a transfer of data from the center to the base, for the base to write the data to an IC card at the base, upon determining that the IC card is authenticated. Laing involves enabling a transfer of data from the center to the base upon determining that the base is authenticated to the center (and/or upon determining that the center

is authenticated to the base). Harada involves enabling a transfer of data from a memory card (i.e., "card") at the base to the base upon determining that the card is authenticated. As such, Laing in combination with Harada lacks enabling a transfer of data from the center to the base upon determining that an IC card (i.e., "card") at the base is authenticated. That is, Harada determines whether a card is authenticated in order to effect transfer of data from the card to a local access point (i.e., the base) as opposed to effect a transfer of data to the card from a remote source point (i.e., the center) as claimed.

Further, the card of Harada is a memory card having data (e.g., an application program) which is to be transferred from the card to the base if the card is authenticated. As such, the card of Harada is not an IC card which is to receive data to be written thereto as claimed.

In summary, the independent claims include features directed to:

(1) enabling a transfer of data from the center to the base upon determining that a card at the base is authenticated; and

(2) the entity at the base that is to be authenticated to enable the data transfer from the center to the base is an IC card which is to receive the data to be written thereto.

Laing in view of Harada, alone or in combination, do not teach or suggest the feature (1) as Laing enables the transfer of data from the center to the base upon determining that the base (and/or the center) is authenticated and Harada enables a transfer of data from a card at the base to the base upon determining that the card is authenticated.

Laing in view of Harada, alone or in combination, do not teach or suggest the feature (2) as the entity in Laing that is to be authenticated to enable the data transfer from the center to the base is the base (and/or the center) as opposed to an IC card at the base as claimed. Likewise, Laing in view of Harada, alone or in combination, do not teach or suggest the feature

(2) as the entity in Harada that is to be authenticated is a card (i.e., memory card) which is to provide data to be read therefrom as opposed to a card (i.e., IC card) which is to receive data from the center to be written thereto by the base as claimed.

In view of the foregoing, independent claims 21, 25, 29, and 33 are patentable under 35 U.S.C. § 103(a) over Laing in view of Harada. Claims 22-24, 26-28, 30-32, and 34-36 depend from one of the independent claims and include the features of their respective independent claim. Thus, claims 22-24, 26-28, 30-32, and 34-36 are also patentable under 35 U.S.C. § 103(a) over Laing in view of Harada.

CONCLUSION

In view of the foregoing, the Applicant respectfully requests the Board to rule that claims 21-36 are patentable under 35 U.S.C. § 103(a) over Laing in view of Harada.

Respectfully submitted,

MASAYOSHI KAWAMOTO et al.

By: /James N. Kallis/
James N. Kallis
Registration No. 41,102
Attorney for Applicant

Date: September 16, 2009

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351

Enclosure - Appendices (pages 1-8)

VIII. CLAIMS APPENDIX

21. A card issuing system for issuing an integrated chip ("IC") card, the card issuing system comprising:

a card issuing center having a center communication means for transmitting card writing data, the card writing data including at least one of a card number and personal information; and

a base having a card communication mediate means for receiving the card writing data from the center communication means via a network, a card writer for receiving an IC card, and a cipher decoding means in communication with the card communication mediate means and the card writer, the cipher decoding means having an access key;

wherein while the card writer receives an IC card having an access key, the cipher decoding means being operable for determining whether the access key of the IC card and the access key of the cipher decoding means correspond to one another and, if the access keys correspond to one another, the cipher decoding means being further operable for enabling the card communication mediate means to receive the card writing data from the center communication means and transmit the received card writing data to the card writer for the card writer to write the card writing data to the IC card such that the card writing data is transmitted from the card issuing center to the IC card without being stored in the base thereby securing security of the at least one of the card number and the personal information of the card writing data.

22. The card issuing system of claim 21 wherein:

the card issuing center further includes a log management database for storing a communication result indicative of the card writing data having been transmitted from the card issuing center to the IC card.

23. The card issuing system of claim 21 wherein:

the card issuing center further includes a control terminal authentication means for determining as a function of authentication information uniquely associated with the card communication mediate means whether the card communication mediate means has authentication to receive card writing data from the center communication means, wherein the control terminal authentication means prevents the center communication means from transmitting card writing data to the card communication mediate means if the card communication mediate means lacks authentication.

24. The card issuing system of claim 21 wherein:

the base further includes a card writer authentication means for determining as a function of authentication information uniquely associated with the card writer whether the card writer has authentication to receive card writing data from the card communication mediate means, wherein the card writer authentication means prevents the card communication mediate means from transmitting card writing data to the card writer if the card writer lacks authentication.

25. A card issuing method for issuing an integrated chip ("IC") card, the card issuing method comprising:

providing a card issuing center having a center communication means for transmitting card writing data, the card writing data including at least one of a card number and personal information;

providing a base having a card communication mediate means for receiving the card writing data from the center communication means via a network, a card writer for receiving an IC card, and a cipher decoding means in communication with the card communication mediate means and the card writer, the cipher decoding means having an access key; and

while the card writer receives an IC card having an access key, determining by the cipher decoding means whether the access key of the IC card and the access key of the cipher decoding means correspond to one another and, if the access keys correspond to one another,

enabling by the cipher decoding means the card communication mediate means to receive the card writing data from the center communication means and transmit the received card writing data to the card writer for the card writer to write the card writing data to the IC card such that the card writing data is transmitted from the card issuing center to the IC card without being stored in the base thereby securing security of the at least one of the card number and the personal information of the card writing data.

26. The card issuing method of claim 25 further comprising:

storing in the card issuing center a communication result indicative of the card writing data having been transmitted from the card issuing center to the IC card.

27. The card issuing method of claim 25 further comprising:

determining as a function of authentication information uniquely associated with the card communication mediate means whether the card communication mediate means has authentication to receive card writing data from the center communication means; and

preventing the center communication means from transmitting card writing data to the card communication mediate means if the card communication mediate means lacks authentication.

28. The card issuing method of claim 25 further comprising:

determining as a function of authentication information uniquely associated with the card writer whether the card writer has authentication to receive card writing data from the card communication mediate means; and

preventing the card communication mediate means from transmitting card writing data to the card writer if the card writer lacks authentication.

29. A card issuing system for issuing an integrated chip ("IC") card, the card issuing system comprising:

a card issuing center having a center communication means for transmitting card writing data, the card writing data including at least one of a card number and personal information; and

a base having a card communication mediate means for receiving the card writing data from the center communication means via a network and a card writer for receiving an IC card;

wherein while the card writer receives an IC card having an access key during a communication connection between the center communication means and the card communication mediate means, the card issuing center being operable for accessing the access key of the IC card and determining whether the IC card is authenticated based on the access key of the IC card and, if the IC card is authenticated, the card issuing center being further operable for enabling the card communication mediate means to receive the card writing data from the center communication means and transmit the received card writing data to the card writer for the card writer to write the card writing data to the IC card such that the card writing data is transmitted from the card issuing center to the IC card without being stored in the base thereby securing security of the at least one of the card number and the personal information of the card writing data.

30. The card issuing system of claim 29 wherein:

the card issuing center further includes a log management database for storing a communication result indicative of the card writing data having been transmitted from the card issuing center to the IC card.

31. The card issuing system of claim 29 wherein:

the card issuing center further includes a control terminal authentication means for determining as a function of authentication information uniquely associated with the card communication mediate means whether the card communication mediate means has authentication to receive card writing data from the center communication means, wherein the

control terminal authentication means prevents the center communication means from transmitting card writing data to the card communication mediate means if the card communication mediate means lacks authentication.

32. The card issuing system of claim 29 wherein:

the base further includes a card writer authentication means for determining as a function of authentication information uniquely associated with the card writer whether the card writer has authentication to receive card writing data from the card communication mediate means, wherein the card writer authentication means prevents the card communication mediate means from transmitting card writing data to the card writer if the card writer lacks authentication.

33. A card issuing method for issuing an integrated chip ("IC") card, the card issuing method comprising:

providing a card issuing center having a center communication means for transmitting card writing data, the card writing data including at least one of a card number and personal information;

providing a base having a card communication mediate means for receiving the card writing data from the center communication means via a network and a card writer for receiving an IC card;

while the card writer receives an IC card having an access key during a communication connection between the center communication means and the card communication mediate means, accessing by the card issuing center the access key of the IC card and determining by the card issuing center whether the IC card is authenticated based on the access key of the IC card and, if the IC card is authenticated, enabling by the card issuing center the card communication mediate means to receive the card writing data from the center communication means and transmit the received card writing data to the card writer for the card writer to write the card writing data to the IC card such that the card writing data is transmitted

from the card issuing center to the IC card without being stored in the base thereby securing security of the at least one of the card number and the personal information of the card writing data.

34. The card issuing method of claim 33 further comprising:

storing in the card issuing center a communication result indicative of the card writing data having been transmitted from the card issuing center to the IC card.

35. The card issuing method of claim 33 further comprising:

determining as a function of authentication information uniquely associated with the card communication mediate means whether the card communication mediate means has authentication to receive card writing data from the center communication means; and

preventing the center communication means from transmitting card writing data to the card communication mediate means if the card communication mediate means lacks authentication.

36. The card issuing method of claim 33 further comprising:

determining as a function of authentication information uniquely associated with the card writer whether the card writer has authentication to receive card writing data from the card communication mediate means; and

preventing the card communication mediate means from transmitting card writing data to the card writer if the card writer lacks authentication.

IX. EVIDENCE APPENDIX

NONE.

X. RELATED PROCEEDINGS APPENDIX

NONE.